(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2003174443 A**

(43) Date of publication of application: **20.06.03**

(51) Int. Cl **H04L 9/08**
G06F 15/00
G06F 17/60
H04L 9/32

(21) Application number: **2001373674**

(22) Date of filing: **07.12.01**

(71) Applicant: **SONY CORP**

(72) Inventor: **ISHII HIDEHIRO**

(54) INFORMATION PROCESSOR AND INFORMATION PROCESSING METHOD, PROGRAM STORAGE MEDIUM, AND PROGRAM

(57) Abstract:

PROBLEM TO BE SOLVED: To freely deliver and distribute contents, and to flexibly set a license for using the contents.

SOLUTION: A contents server encrypts contents in providing the contents via the Internet to a client. Then, attribute information associated with the contents is described in the header of the encrypted contents. The client acquires a license to permit the encrypted contents by performing an access to a license server to acquire a license where the attribute information of the contents fulfills an attribute condition.

COPYRIGHT: (C)2003,JPO

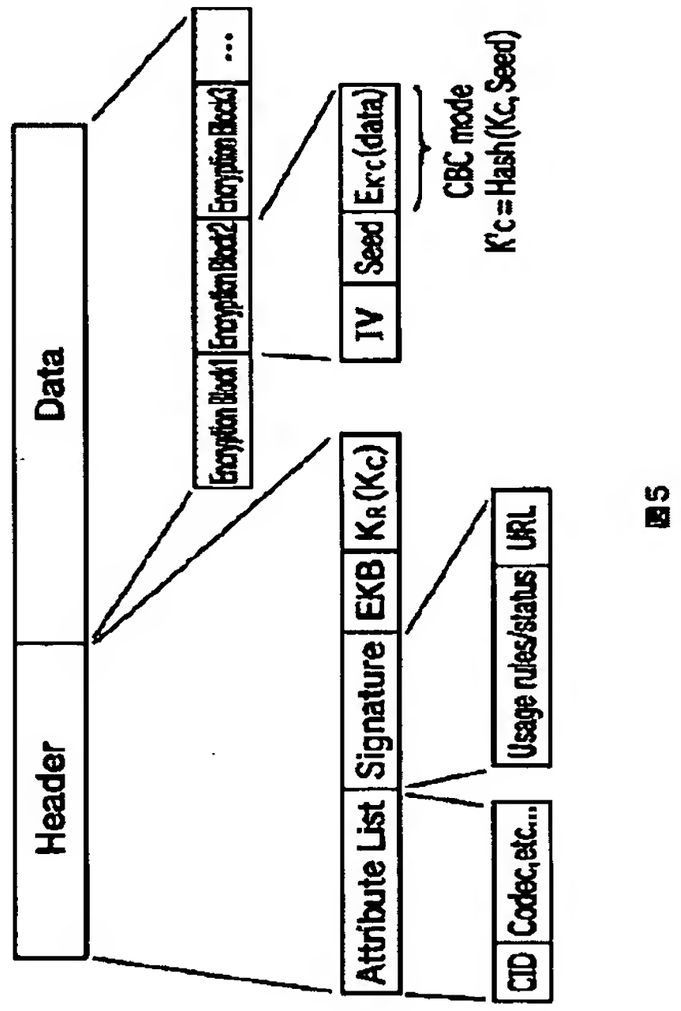

図5

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2003－174443
(P2003－174443A)
(43)公開日　平成15年６月20日(2003.6.20)

(51)Int.Cl.'		識別記号	FI		テーマコード'(参考)
Ｈ０４Ｌ	9/08		Ｇ０６Ｆ	15/00	３３０Ｚ　５Ｂ０８５
Ｇ０６Ｆ	15/00	３３０		17/60	１４２　５Ｊ１０４
	17/60	１４２			３０２Ｅ
		３０２	Ｈ０４Ｌ	9/00	６０１Ｂ
Ｈ０４Ｌ	9/32				６７３Ｚ

審査請求　有　請求項の数11　ＯＬ　（全 18 頁）

(21)出願番号　特願2001－373674(P2001－373674)

(22)出願日　平成13年12月７日(2001.12.7)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　石井　秀浩
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100082131
弁理士　稲本　義雄

Ｆターム(参考)　5B085 AE23 AE29 BA07 BG03 BG07
5J104 AA09 AA13 AA16 PA07

(54)【発明の名称】　情報処理装置および方法、プログラム格納媒体、並びにプログラム

(57)【要約】
【課題】　コンテンツを自由に配布・流通させつつ、それを利用するためのライセンスを柔軟に設定できるようにする。
【解決手段】　コンテンツサーバは、クライアントにインターネットを介してコンテンツを提供するとき、コンテンツを暗号化する。その暗号化されたコンテンツのヘッダには、そのコンテンツに関する属性情報が記述される。クライアントは、コンテンツの属性情報が属性条件を満たすようなライセンスをライセンスサーバにアクセスして取得することで、暗号化されたコンテンツを許可するライセンスを取得する。

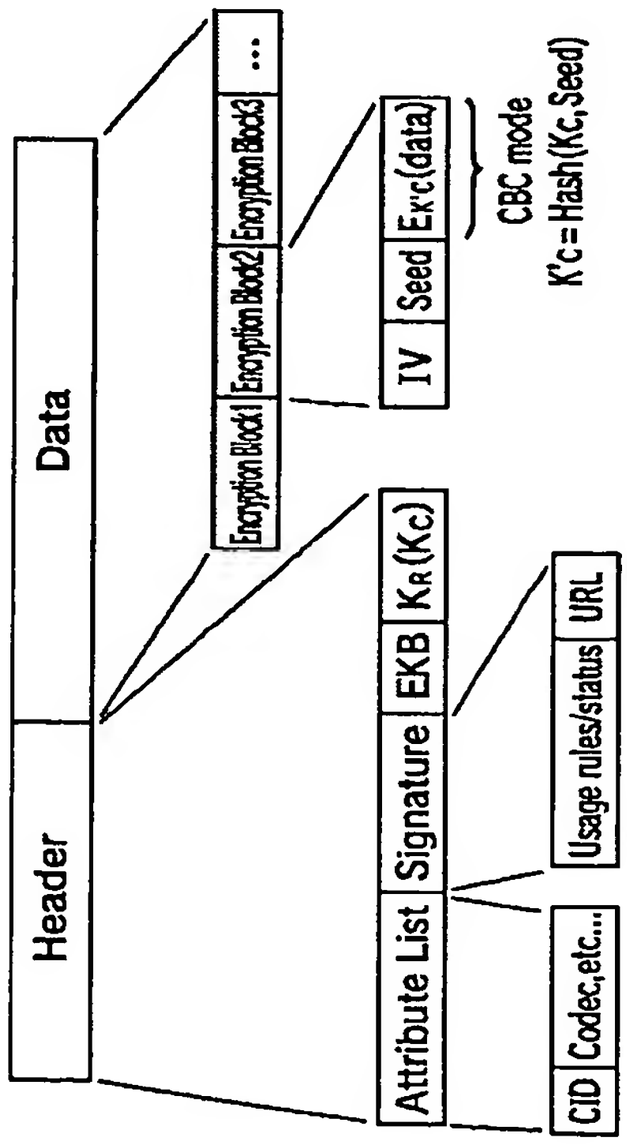

図5

【特許請求の範囲】
【請求項１】　暗号化コンテンツデータと属性情報とを含むコンテンツを受信するコンテンツ受信手段と、
前記コンテンツを記憶するコンテンツ記憶手段と、
利用できるコンテンツの前記属性情報に関する条件を記載した属性条件を含むライセンスを受信するライセンス受信手段と、
前記ライセンスを記憶するライセンス記憶手段と、
前記ライセンス記憶部に記憶されているライセンスが、前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすか否かを判定する判定手段と、
前記判定手段が前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすと判定したことに基づいて、前記コンテンツの前記暗号化コンテンツデータを復号する復号手段と、
前記復号手段により復号されたコンテンツデータを出力する出力手段と、を備えることを特徴とする情報処理装置。
【請求項２】　前記コンテンツは、更に前記コンテンツデータを復号するためのコンテンツキーを含む、
ことを特徴とする請求項１記載の情報処理装置。
【請求項３】　前記属性情報は、属性項目と属性値の組み合わせからなる、ことを特徴とする請求項１記載の情報処理装置。
【請求項４】　前記属性項目はレコード会社、アーティスト、リリース日、コンテンツ発行者、ジャンル、サブスクリプション、またはレーベルに関する情報により規定される、
ことを特徴とする請求項１記載の情報処理装置。
【請求項５】　前記属性条件は属性項目、属性値、及び演算子の組み合わせからなる、
ことを特徴とする請求項１記載の情報処理装置。
【請求項６】　コンテンツに含まれる属性情報に関する条件を記載した属性条件を含むライセンスを一意に識別するライセンスIDを含むライセンス要求を受信する受信手段と、
ライセンスをライセンスIDと共に記憶する記憶手段と、
前記ライセンス要求に含まれる前記ライセンスIDに対応する前記ライセンスを取り込む取り込み手段と、
前記ライセンスに電子署名を付加する署名手段と、
署名手段により署名されたライセンスを送信する送信手段と、を備えることを特徴とする情報処理装置。
【請求項７】　更に、前記取り込み手段によって取り込まれたライセンスに端末IDを付加するライセンス処理手段、
を備えることを特徴とする請求項６記載の情報処理装置。
【請求項８】　暗号化コンテンツデータと属性情報とを含むコンテンツを記憶する記憶手段と、
コンテンツを一意に識別するコンテンツIDを含むコンテンツ要求を受信する受信手段と、
コンテンツ要求に含まれるコンテンツIDに対応するコンテンツを送信する送信手段と、
を備える情報処理装置であって、
前記コンテンツに含まれる前記属性情報は、当該コンテンツを利用する際にライセンスの属性条件を満たすか否かを判断するために用いられる情報であり、
前記ライセンスの属性条件は利用できる前記コンテンツの前記属性情報に関する条件を記載した情報である、
ことを特徴とする情報処理装置。
【請求項９】　暗号化コンテンツデータと属性情報とを含むコンテンツを受信するコンテンツ受信ステップと、
前記コンテンツを記憶するコンテンツ記憶ステップと、
利用できるコンテンツの前記属性情報に関する条件を記載した属性条件を含むライセンスを受信するライセンス受信ステップと、
前記ライセンスを記憶するライセンス記憶ステップと、
前記ライセンス記憶部に記憶されているライセンスが、前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすか否かを判定する判定ステップと、
前記判定手段が前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすと判定したことに基づいて、前記コンテンツの前記暗号化コンテンツデータを復号する復号ステップと、
前記復号手段により復号されたコンテンツデータを出力する出力ステップと、を含むことを特徴とする情報処理方法。
【請求項１０】　暗号化コンテンツデータと属性情報とを含むコンテンツを受信するコンテンツ受信ステップと、
前記コンテンツを記憶するコンテンツ記憶ステップと、
利用できるコンテンツの前記属性情報に関する条件を記載した属性条件を含むライセンスを受信するライセンス受信ステップと、
前記ライセンスを記憶するライセンス記憶ステップと、
前記ライセンス記憶部に記憶されているライセンスが、前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすか否かを判定する判定ステップと、
前記判定手段が前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすと判定したことに基づいて、前記コンテンツの前記暗号化コンテンツデータを復号する復号ステップと、
前記復号手段により復号されたコンテンツデータを出力する出力ステップと、
をコンピュータに実行させるプログラム。
【請求項１１】　暗号化コンテンツデータと属性情報とを含むコンテンツを受信するコンテンツ受信ステップと、
前記コンテンツを記憶するコンテンツ記憶ステップと、
利用できるコンテンツの前記属性情報に関する条件を記

載した属性条件を含むライセンスを受信するライセンス受信ステップと、
前記ライセンスを記憶するライセンス記憶ステップと、
前記ライセンス記憶部に記憶されているライセンスが、前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすか否かを判定する判定ステップと、
前記判定手段が前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすと判定したことに基づいて、前記コンテンツの前記暗号化コンテンツデータを復号する復号ステップと、
前記復号手段により復号されたコンテンツデータを出力する出力ステップと、をコンピュータに実行させるプログラムが格納されたプログラム格納媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、情報処理装置および方法、プログラム格納媒体、並びにプログラムに関し、特に、著作権者からライセンスを受けていないコンテンツが不正にコピーされ、利用されるのを防止することができるようにした、情報処理装置および方法、プログラム格納媒体、並びにプログラムに関する。

【０００２】

【従来の技術】最近、インターネットを介して、ユーザが、自分自身が保持している音楽データを他のユーザに提供し、自分自身が保持していない音楽データを他のユーザから提供を受けるようにして、複数のユーザが無料で音楽データを交換しあうシステムが実現されている。

【０００３】このようなシステムでは、理論的には、１つの音楽、その他のコンテンツが存在すれば、他の全てのユーザが、それを利用することが可能となり、多くのユーザがコンテンツを購入しなくなるため、コンテンツに関する著作権者は、著作物としてのコンテンツが売れないため、著作物の販売に伴い、本来受け取ることが可能な著作物の利用に関するロイヤリティを受け取る機会を失うことになる。

【０００４】そこで、配布されるコンテンツは暗号化しておき、そのコンテンツを利用するためのライセンスを別途発行し、暗号化されたコンテンツに対応するライセンスを持っていないとコンテンツを復号、再生できないようにするようにしたシステムがある。

【０００５】このようにすることでコンテンツを自由に配布することを可能としつつ、著作物の著作権を保護することができる。

【０００６】

【発明が解決しようとする課題】しかしながら、上記のシステムでは、ライセンスとコンテンツの対応関係を柔軟に設定したり、既に配布されたライセンスよって利用できるコンテンツを新たに配布することが難しかった。

【０００７】本発明はこのような状況に鑑みてなされたものであり、コンテンツは自由に配布・流通させ、ライセンスによって利用できるコンテンツの集合を自由に設定することができるようにするものである。

【０００８】

【課題を解決するための手段】本発明の第１の情報処理装置は、暗号化コンテンツデータと属性情報とを含むコンテンツを受信するコンテンツ受信手段と、前記コンテンツを記憶するコンテンツ記憶手段と、利用できるコンテンツの前記属性情報に関する条件を記載した属性条件を含むライセンスを受信するライセンス受信手段と、前記ライセンスを記憶するライセンス記憶手段と、前記ライセンス記憶部に記憶されているライセンスが、前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすか否かを判定する判定手段と、前記判定手段が前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすと判定したことに基づいて、前記コンテンツの前記暗号化コンテンツデータを復号する復号手段と、前記復号手段により復号されたコンテンツデータを出力する出力手段とを備えることを特徴とする。

【０００９】前記コンテンツは、更に前記コンテンツデータを復号するためのコンテンツキーを含むようにすることができる。

【００１０】前記属性情報は、属性項目と属性値の組み合わせから構成することができる。

【００１１】前記属性項目はレコード会社、アーティスト、リリース日、コンテンツ発行者、ジャンル、サブスクリプション、またはレーベルに関する情報により規定することができる。

【００１２】前記属性条件は属性項目、属性値、及び演算子の組み合わせから構成することができる。

【００１３】本発明の第２の情報処理装置は、コンテンツに含まれる属性情報に関する条件を記載した属性条件を含むライセンスを一意に識別するライセンスIDを含むライセンス要求を受信する受信手段と、ライセンスをライセンスIDと共に記憶する記憶手段と、前記ライセンス要求に含まれる前記ライセンスIDに対応する前記ライセンスを取り込む取り込み手段と、前記ライセンスに電子署名を付加する署名手段と、署名手段により署名されたライセンスを送信する送信手段とを備えることを特徴とする。

【００１４】更に、前記取り込み手段によって取り込まれたライセンスに端末IDを付加するライセンス処理手段を備えることができる。

【００１５】本発明の第３の情報処理装置は、暗号化コンテンツデータと属性情報とを含むコンテンツを記憶する記憶手段と、コンテンツを一意に識別するコンテンツIDを含むコンテンツ要求を受信する受信手段と、コンテンツ要求に含まれるコンテンツIDに対応するコンテンツを送信する送信手段とを備える情報処理装置であって、前記コンテンツに含まれる前記属性情報は、当該コンテンツを利用する際にライセンスの属性条件を満たすか否

かを判断するために用いられる情報であり、前記ライセンスの属性条件は利用できる前記コンテンツの前記属性情報に関する条件を記載した情報であることを特徴とする。

【００１６】本発明の情報処理方法は、暗号化コンテンツデータと属性情報とを含むコンテンツを受信するコンテンツ受信ステップと、前記コンテンツを記憶するコンテンツ記憶ステップと、利用できるコンテンツの前記属性情報に関する条件を記載した属性条件を含むライセンスを受信するライセンス受信ステップと、前記ライセンスを記憶するライセンス記憶ステップと、前記ライセンス記憶部に記憶されているライセンスが、前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすか否かを判定する判定ステップと、前記判定手段が前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすと判定したことに基づいて、前記コンテンツの前記暗号化コンテンツデータを復号する復号ステップと、前記復号手段により復号されたコンテンツデータを出力する出力ステップとを含むことを特徴とする。

【００１７】本発明のプログラムは、暗号化コンテンツデータと属性情報とを含むコンテンツを受信するコンテンツ受信ステップと、前記コンテンツを記憶するコンテンツ記憶ステップと、利用できるコンテンツの前記属性情報に関する条件を記載した属性条件を含むライセンスを受信するライセンス受信ステップと、前記ライセンスを記憶するライセンス記憶ステップと、前記ライセンス記憶部に記憶されているライセンスが、前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすか否かを判定する判定ステップと、前記判定手段が前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすと判定したことに基づいて、前記コンテンツの前記暗号化コンテンツデータを復号する復号ステップと、前記復号手段により復号されたコンテンツデータを出力する出力ステップとをコンピュータに実行させるプログラムである。

【００１８】本発明のプログラム格納媒体に格納されているプログラムは、暗号化コンテンツデータと属性情報とを含むコンテンツを受信するコンテンツ受信ステップと、前記コンテンツを記憶するコンテンツ記憶ステップと、利用できるコンテンツの前記属性情報に関する条件を記載した属性条件を含むライセンスを受信するライセンス受信ステップと、前記ライセンスを記憶するライセンス記憶ステップと、前記ライセンス記憶部に記憶されているライセンスが、前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすか否かを判定する判定ステップと、前記判定手段が前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすと判定したことに基づいて、前記コンテンツの前記暗号化コンテンツデータを復号する復号ステップと、前記復号手段により復号されたコンテンツデータを出力する出力ステップとをコンピュータに実行させるプログラムである。

【００１９】

【発明の実施の形態】図１は、本発明を適用したコンテンツ提供システムの構成を示している。インターネット２には、クライアント１－１，１－２（以下、これらのクライアントを個々に区別する必要がない場合、単にクライアント１と称する）が接続されている。この例においては、クライアントが２台のみ示されているが、インターネット２には、任意の台数のクライアントが接続される。

【００２０】また、インターネット２には、クライアント１に対してコンテンツを提供するコンテンツサーバ３、コンテンツサーバ３が提供するコンテンツを利用するのに必要なライセンスをクライアント１に対して付与するライセンスサーバ４、およびクライアント１がライセンスを受け取った場合に、そのクライアント１に対して課金処理を行う課金サーバ５が接続されている。

【００２１】これらのコンテンツサーバ３、ライセンスサーバ４、および課金サーバ５も、任意の台数、インターネット２に接続される。

【００２２】図２はクライアント１の構成を表している。

【００２３】図２において、CPU（Central Processing Unit）２１は、ROM（Read Only Memory）２２に記憶されているプログラム、または記憶部２８からRAM（Random Access Memory）２３にロードされたプログラムに従って各種の処理を実行する。タイマ２０は、計時動作を行い、時刻情報をCPU２１に供給する。RAM２３にはまた、CPU２１が各種の処理を実行する上において必要なデータなども適宜記憶される。

【００２４】暗号化復号部２４は、コンテンツデータを暗号化するとともに、既に暗号化されているコンテンツデータを復号する処理を行う。コーデック部２５は、例えば、ATRAC（Adaptive Transform Acoustic Coding）３方式などでコンテンツデータをエンコードし、入出力インタフェース３２を介してドライブ３０に接続されている半導体メモリ４４に供給し、記録させる。あるいはまた、コーデック部２５は、ドライブ３０を介して半導体メモリ４４より読み出した、エンコードされているデータをデコードする。

【００２５】半導体メモリ４４は、例えば、メモリスティック（商標）などにより構成される。

【００２６】CPU２１、ROM２２、RAM２３、暗号化復号部２４、およびコーデック部２５は、バス３１を介して相互に接続されている。このバス３１にはまた、入出力インタフェース３２も接続されている。

【００２７】入出力インタフェース３２には、キーボード、マウスなどよりなる入力部２６、CRT、LCDなどよりなるディスプレイ、並びにスピーカなどよりなる出力部２７、ハードディスクなどより構成される記憶部２８、

モデム、ターミナルアダプタなどより構成される通信部２９が接続されている。通信部２９は、インターネット２を介しての通信処理を行う。通信部２９はまた、他のクライアントとの間で、アナログ信号またはデジタル信号の通信処理を行う。

【００２８】入出力インタフェース３２にはまた、必要に応じてドライブ３０が接続され、磁気ディスク４１、光ディスク４２、光磁気ディスク４３、或いは半導体メモリ４４などが適宜装着され、それらから読み出されたコンピュータプログラムが、必要に応じて記憶部２８にインストールされる。

【００２９】なお、図示は省略するが、コンテンツサーバ3、ライセンスサーバ4、課金サーバ5も、図２に示したクライアント１と基本的に同様の構成を有するコンピュータにより構成される。

【００３０】次に、図３のフローチャートを参照して、クライアント１がコンテンツサーバ３からコンテンツの提供を受ける処理について説明する。

【００３１】ユーザが、入力部２６を操作することでコンテンツサーバ３に対するアクセスを指令すると、CPU２１は、通信部２９を制御し、インターネット２を介してコンテンツサーバ３にアクセスさせる。ステップＳ２において、ユーザが、入力部２６を操作して、提供を受けるコンテンツを指定すると、CPU２１は、この指定情報を受け取り、通信部２９から、インターネット２を介してコンテンツサーバ３に、指定されたコンテンツを通知する。図４のフローチャートを参照して後述するように、この通知を受けたコンテンツサーバ３は、暗号化されたコンテンツデータを送信してくるので、ステップＳ３において、CPU２１は、通信部２９を介して、このコンテンツデータを受信すると、ステップＳ４において、その暗号化されているコンテンツデータを記憶部２８を構成するハードディスクに供給し、記憶させる。

【００３２】次に、図４のフローチャートを参照して、クライアント１の以上の処理に対応するコンテンツサーバ３のコンテンツ提供処理について説明する。なお、以下の説明において、図２のクライアント１の構成は、コンテンツサーバ３の構成としても引用する。

【００３３】ステップＳ２１において、コンテンツサーバ３のCPU２１は、インターネット２から通信部２９を介してクライアント１よりアクセスを受けるまで待機し、アクセスを受けたと判定したとき、ステップＳ２２に進み、クライアント１から送信されてきたコンテンツを指定する情報を取り込む。このコンテンツを指定する情報は、クライアント１が、図３のステップＳ２において通知してきた情報である。

【００３４】ステップＳ２３において、コンテンツサーバ３のCPU２１は、記憶部２８に記憶されているコンテンツデータの中から、ステップＳ２２の処理で取り込まれた情報で指定されたコンテンツを読み出す。CPU２１は、ステップＳ２４において、記憶部２８から読み出されたコンテンツデータを、暗号化復号部２４に供給し、暗号化させる。

【００３５】記憶部２８に記憶されているコンテンツデータは、コーデック部２５により、既にATRAC３方式によりエンコードされているので、このエンコードされているコンテンツデータが暗号化されることになる。

【００３６】なお、もちろん、記憶部２８に予め暗号化した状態でコンテンツデータを記憶させることができる。この場合には、ステップＳ２４の処理は省略することが可能である。

【００３７】次に、ステップＳ２５において、コンテンツサーバ３のCPU２１は、暗号化したコンテンツデータを伝送するフォーマットを構成するヘッダに、暗号化されているコンテンツを復号するのに必要なキーと、コンテンツに関する各種情報を示す属性情報を付加する。そして、ステップＳ２６において、コンテンツサーバ３のCPU２１は、ステップＳ２４の処理で暗号化したコンテンツと、ステップＳ２５の処理でキーと属性情報及びその電子署名を付加したヘッダとをフォーマット化したデータを、通信部２９から、インターネット２を介して、アクセスしてきたクライアント１に送信する。

【００３８】図５は、このようにして、コンテンツサーバ３からクライアント１にコンテンツが供給される場合のフォーマットの構成を表している。同図に示されるように、このフォーマットは、ヘッダ（Header）とデータ（Data）とにより構成される。

【００３９】ヘッダには、属性情報（Attribute List）及び属性情報をライセンスサーバの暗号鍵で署名した電子署名、イネーブリングキーブロック（EKB（Enabling KeyBlock））および、EKBをDNKを用いて復号処理することによって得られるルートキーKRにより暗号化されたコンテンツキーKc（KR（Kc））が配置されている。

【００４０】属性情報には属性項目と属性値との組み合わせからなる属性のエントリーが複数記述されている。

【００４１】属性項目の種類を図６に示す。CID、RCID、CIID、AID、GID及びLIDはそれぞれコンテンツ、レコード会社、コンテンツ発行者、アーティスト、ジャンル及びレーベルを一意に識別するIDである。RelDateはコンテンツのリリース日を表す。サブスクリプションIDは後述するサブスクリプションライセンスに用いられる属性項目である。

【００４２】URLは、コンテンツを利用するためのライセンスを取得するときアクセスするアドレス情報であり、図１のシステムの場合、具体的には、ライセンスを受けるために必要なライセンスサーバ４のアドレスである。

【００４３】データは、任意の数の暗号化ブロック（Encryption block）により構成される。各暗号化ブロックは、イニシャルベクトル（IV（Initial Vector））、シ

ード（Seed）、およびコンテンツデータをキーK'cで暗号化したデータEK'c(data)により構成されている。

【００４４】キーK'cは、次式により示されるように、コンテンツキーKcと、乱数で設定される値Seedをハッシュ関数に適応して演算された値により構成される。

【００４５】K'c＝Hash(Kc, Seed)

【００４６】イニシャルベクトルIVとシードSeedは、各暗号化ブロック毎に異なる値に設定される。

【００４７】この暗号化は、コンテンツのデータを８バイト単位で区分して、８バイト毎に行われる。後段の８バイトの暗号化は、前段の８バイトの暗号化の結果を利用して行われるCBC（Cypher Block Chaning）モードで行われる。

【００４８】CBCモードの場合、最初の８バイトのコンテンツデータを暗号化するとき、その前段の８バイトの暗号化結果が存在しないため、最初の８バイトのコンテンツデータを暗号化するときは、イニシャルベクトルIVを初期値として暗号化が行われる。

【００４９】このCBCモードによる暗号化を行うことで、１つの暗号化ブロックが解読されたとしても、その影響が、他の暗号化ブロックにおよぶことが抑制される。

【００５０】なお、この暗号化については、図１４と図１５を参照にして、後に詳述する。

【００５１】以上のようにして、クライアント１は、コンテンツサーバ３からコンテンツを無料で、自由に取得することができる。

【００５２】しかしながら、各クライアント１は、取得したコンテンツを利用するとき、ライセンスを取得する必要がある。

【００５３】ライセンスを取得する際には、クライアント１は事前にライセンスサーバにオンラインあるいはオフラインで登録処理を行い、サービスデータを取得しておく。サービスデータにはデバイスノードキー（DNK）及び端末IDが含まれており、EKBを復号処理するのに用いられる。サービスデータ及びライセンスサーバから取得するライセンスはクライアント１の記憶部２８にセキュアに保存される。

【００５４】図７にライセンスの構成を示す。ライセンスにはライセンスID、タイムスタンプ、使用期限、属性条件、使用規則、及びこれらをライセンスサーバの秘密鍵で署名した電子署名が含まれる。タイムスタンプはライセンスの発行日を表す。使用期限はライセンスを使用できる期限日を表し、この期限日を過ぎるとそのライセンスは使用できなくなる。属性条件はそのライセンスを所持しているクライアント１が利用できるコンテンツの属性の条件を属性項目と属性項目に関する値、比較演算子、及び論理演算子の組み合わせからなる条件式によって表したものである。使用規則にはそのライセンスの利用できるコンテンツを使用するための規則を記述したものであり、サービスデータに含まれているものと同じ端末IDが含まれる。

【００５５】以下に、コンテンツに含まれる属性情報、及びライセンスに含まれる属性条件との組み合わせによって実現可能なライセンス構成の例を示す。

【００５６】コンテンツc1の属性情報には、次のように記述されている。

c1: cid = {1}, aid = {0, 1}, reldate = 2000年11月10日

【００５７】これは、コンテンツIDは1、アーティストIDは0および1（即ち、0番のアーティストと1番のアーティストの合作）、リリース日は2000年11月10日であるということを表す。

【００５８】同様に、コンテンツc2, c3, c4の属性情報に、次のように記述されている。

c2: cid = {2}, aid = {0}, reldate = 2000年12月20日
c3: cid = {3}, aid = {0}, reldate = 2001年3月1日
c4: cid = {4}, aid = {0}, reldate = 2001年10月21日

一方、ライセンスl1の属性条件には、次のように記述されている。

l1: cid ∋ 1 ∨ cid ∋ 2

【００５９】これにより、利用権r1はコンテンツc1とc2に対応する。即ち、利用権r1が有効な端末では、コンテンツc1とc2を利用する事ができる。

【００６０】ライセンスl2の属性条件は、次のように記述されている。

l2: aid ∋ 0 ∧ (2001年1月1日 < reldate < 2001年12月31日)

【００６１】これは、2001年にリリースされた0番のアーティストのコンテンツ、という意味の条件であり、ライセンスl2はコンテンツc3とc4に対応する。この時点で、ライセンスl2が有効な端末では、コンテンツc3とc4を利用する事ができる。後に下記のような属性情報を持たせたコンテンツc5が発行されたとする。

c5: cid = {5}, aid = {0}, reldate = {2001年12月1日}

【００６２】このコンテンツをコンテンツサーバ３からダウンロードするなどして入手すると、既にライセンスl2を保有しているクライアント１では、新たにライセンスサーバ等に接続する必要なく、コンテンツc5も利用できるようになる。

【００６３】これらのコンテンツの配布後、配信事業者が新たにベスト版としてコンテンツc1, c2, c5を組み合わせて発売しようとするならば、それに対応する次のようなライセンスl3を発行すれば、コンテンツを新たに作成する必要なく、配布済み・流通中のコンテンツをそのまま活用して、ベスト版発売が可能である。

l3: cid ∋ 1 ∨ cid ∋ 2 ∨ cid ∋ 5

【００６４】このようにして、配布済み・流通中のコンテンツを組み合わせた利用権を容易に新規発行できる。

例えば、リリース日とアーティストを制約した属性条件を持つライセンスを発行することで、1990年～1999年の谷村新司全集を新たに発売することができる。

【００６５】また、アーティストを制約した属性条件を持つライセンスを発行することで、モーニング娘ファミリー全集（モーニング娘、プッチモニ、中澤裕子、他関連アーティストのコンテンツを集めたもの）を新たに発売することができる。

【００６６】また、The Alfee Best（例えばコンテンツIDを制約する）。

【００６７】次に、サブスクリプション・サービスとして、毎月いくつかの新譜を追加利用できるようになるライセンスを定義する例を示す。

【００６８】ライセンスl4の属性の条件を、次のように定義する。

l4: cid ∋ 3 ∨ cid ∋ 4 ∨ sid ∋ 1

【００６９】このライセンスl4を所持しているクライアント１では、まず、既に発行されているコンテンツc3とc4が利用可能である。翌月、新譜として次のような属性情報を持ったコンテンツc6とc7が発行されたとする。

c6: cid = {6}, sid = {1}

c7: cid = {7}, sid = {1}

【００７０】この場合、ライセンスl4を持っているクライアント１は、新たにライセンスを購入する必要なく、コンテンツc6とc7を利用する事ができる。同様にして、月ごとにサブスクリプションIDに1を含んだコンテンツを発行する事により、ライセンスl4を持っているクライアント１はライセンスを別途購入することなく、利用可能なコンテンツを追加していく事ができる。

【００７１】このように、属性条件を属性項目、属性値、及び論理演算子、関係演算子等の演算子の組み合わせで表すことで、利用できるコンテンツの集合を柔軟に設定できるようになる。

【００７２】属性条件に含まれる演算子はここに挙げられているに限定されず、その他の各種演算子を利用することができる。

【００７３】図８を参照して、クライアント１がコンテンツを再生する場合の処理について説明する。

【００７４】ステップＳ４１において、クライアント１のCPU２１は、ユーザが入力部２６を操作することで指示したコンテンツIDを取得する。

【００７５】そして、CPU２１は、コンテンツIDを取得すると該当するコンテンツデータのヘッダに記述されている属性情報を読み取る。

【００７６】次に、ステップＳ４２に進み、CPU２１は、ステップＳ４１で読み取られた属性情報が各ライセンスに記述されている利用コンテンツ条件式を満たすライセンスが、クライアント１により既に取得され、記憶部２８に記憶されているか否かを判定する。そのようなライセンスが見つからなかった場合には、ステップＳ４３に進み、ＣＰＵ２１は、出力部２７を介して、ディスプレイにライセンスの取得を促すメッセージを表示する。

【００７７】ステップＳ４２において、ライセンスが既に取得されていると判定された場合、ステップＳ４４に進み、CPU２１は、取得されているライセンスは有効期限内のものであるか否かを判定する。ライセンスが有効期限内のものであるか否かは、ライセンスの内容として規定されている期限と、タイマ２０により計時されている現在日時と比較することがで判断される。ライセンスの有効期限が既に満了していると判定された場合、CPU２１は、ステップＳ４５に進み、ライセンス更新処理を実行する。このライセンス更新処理の詳細は、図８のフローチャートを参照して後述する。

【００７８】ステップＳ４４において、ライセンスはまだ有効期限内であると判定された場合、または、ステップＳ４５において、ライセンスが更新された場合、ステップＳ４５’に進み、CPU２１は、コンテンツのヘッダに含まれる電子署名及びライセンスに含まれる電子署名をライセンスサーバ４の公開鍵で検証する。電子署名の検証の結果、電子署名が正しいと判断された場合、ステップＳ４６に進み、CPU２１は、暗号化されているコンテンツデータを記憶部２８から読み出し、RAM２３に格納させる。そして、ステップＳ４７において、CPU２１は、RAM２３に記憶された暗号化ブロックのデータを、図５のデータに配置されている暗号化ブロック単位で、暗号化復号部２４に供給し、復号させる。

【００７９】CPU２１は、さらに、ステップＳ４８において、暗号化復号部２４により復号されたコンテンツデータをコーデック部２５に供給し、デコードさせる。そして、コーデック部２５によりデコードされたデータを、CPU２１は、入出力インタフェース３２から出力部２７に供給し、D/A変換させ、スピーカから出力させる。

【００８０】図９～図11を用いてクライアントがライセンスサーバ４からライセンスを所得する処理を説明する。

【００８１】図９はクライアント１のユーザが利用したいコンテンツが決まっている場合のライセンス取得処理を示している。ユーザが、入力部２６を操作することでコンテンツを指定しライセンスサーバ４にライセンスリストの要求を指示すると、CPU２１は、通信部２９を制御し、インターネット２を介してコンテンツサーバ３に指定されたコンテンツのコンテンツIDを含むライセンスリスト要求を送信する。ライセンスサーバ４はライセンスリスト要求を受信すると、受信したライセンスリストに含まれるコンテンツIDから、該当するコンテンツを利用可能なライセンスを抽出し、各ライセンスのライセンスID、ライセンス名、利用できるコンテンツの条件、現在利用できるコンテンツのリスト、コンテンツの使用条

件等を記載したライセンスリストをクライアント１に送信する。

【００８２】クライアント１がライセンスサーバ４からライセンスリストを受信すると、CPU２１は、出力部２７にライセンスリストに含まれる各ライセンスの情報を表示する。ユーザがその情報を参照し、所望するライセンスを選択すると、CPU２１は、通信部２９を制御し、SSLなどの相互認証によりセッションを形成した後、インターネット２を介してコンテンツサーバ３に、選択されたライセンスのライセンスIDと端末IDと課金用のユーザID及びパスワードを含むライセンス要求を暗号化して送信する。ライセンスサーバ４はクライアント１から送信されたライセンス要求を受信すると、後述するライセンス発行処理を行った後、ライセンス要求に含まれるライセンスIDに対応するライセンスをクライアント１に送信する。クライアント１はライセンスサーバ４から送信されたライセンスを受信すると、受信したライセンスを暗号化等をしてセキュアな状態で記憶部２８に保存する。

【００８３】以上のようにして、ユーザはクライアント１が既に所持しているコンテンツを利用するためのライセンスを取得することができる。以上のライセンス取得処理は、ユーザがクライアントに所持しているコンテンツを再生する操作した際に、そのコンテンツを再生するためのライセンスを取得していなかった場合、自動的に開始されるようにしても良い。

【００８４】次に、ユーザが各種検索条件を指定してライセンスを検索し、取得する処理を図１６に示す。まず、ユーザが欲しいライセンスを検索するための、ライセンス名、ライセンスの種類、ライセンスが利用可能とするコンテンツのタイトル、アルバム名、ジャンル、アーティスト名、リリース日等の検索条件を入力部２６を操作することによって指定すると、CPU２１は、通信部を制御し、入力された検索条件をフォーマットしたデータを含むライセンスリスト要求をコンテンツサーバ３に送信する。コンテンツサーバはクライアント１から送信されたライセンスリスト要求を受信すると、ライセンスリスト要求に含まれる検索条件を満たすライセンスを記憶部２８から検索し、ライセンスID等の各ライセンスに関する情報を含むライセンスリストをクライアント１に送信する。

【００８５】クライアント１がライセンスサーバ４からライセンスリストを受信すると、CPU２１は、出力部２７にライセンスリストに含まれる各ライセンスの情報を表示する。ユーザがその情報を参照し、所望するライセンスを選択すると、CPU２１は、通信部２９を制御し、SSLなどの相互認証によりセッションを形成した後、インターネット２を介してコンテンツサーバ３に、選択されたライセンスのライセンスIDと端末IDと課金用のユーザID及びパスワードを含むライセンス要求を暗号化して送信する。ライセンスサーバ４はクライアント１から送信されたライセンス要求を受信すると、後述するライセンス発行処理を行った後、ライセンス要求に含まれるライセンスIDに対応するライセンスをクライアント１に送信する。クライアント１はライセンスサーバ４から送信されたライセンスを受信すると、受信したライセンスを暗号化するなどしてセキュアな状態で記憶部２８に保存する。

【００８６】以上のようにして、ユーザは欲しいライセンスを検索し、取得することができる。

【００８７】次に、ユーザが欲しいライセンスのライセンスIDを知っている場合のライセンス取得処理を図11に示す。

【００８８】ユーザがライセンスIDを入力部２６を操作し入力して、欲しいライセンスのライセンスIDを指定すると、CPU２１は、通信部２９を制御し、SSLなどの相互認証によりセッションを形成した後、インターネット２を介してコンテンツサーバ３に、選択されたライセンスのライセンスIDと端末IDと課金用のユーザID及びパスワードを含むライセンス要求を暗号化して送信する。ライセンスサーバ４はクライアント１から送信されたライセンス要求を受信すると、後述するライセンス発行処理を行った後、ライセンス要求に含まれるライセンスIDに対応するライセンスをクライアント１に送信する。クライアント１はライセンスサーバ４から送信されたライセンスを受信すると、受信したライセンスを暗号化等をしてセキュアな状態で記憶部２８に保存する。

【００８９】以上のようにして、ユーザは雑誌などに記載されているライセンスの広告などからライセンスIDを知り、そのライセンスIDを指定することで所望するライセンスを取得することができる。

【００９０】また、WebサイトのHTMLファイルや電子メール等にライセンスＩＤを含むライセンスサーバのURLのリンク情報が記載されており、これをユーザがクリックするなどして選択することでライセンス取得処理を開始するようにしても良い。

【００９１】図12のフローチャートを参照して、で図９～図11におけるライセンス発行処理の詳細を説明する。なお、この場合においても、図２のクライアント１の構成は、ライセンスサーバ４の構成としても引用される。

【００９２】最初にステップＳ１０２において、CPU２１はライセンス要求に含まれるライセンスID、端末ID、ユーザID、パスワードを取り込む。

【００９３】そして、ライセンスサーバ４のCPU２１は、通信部２９から課金サーバ５にアクセスし、ユーザIDとパスワードに対応するユーザの与信処理を要求する。課金サーバ５は、インターネット２を介してライセンスサーバ４から与信処理の要求を受けると、そのユーザIDとパスワードに対応するユーザの過去の支払い履歴などを調査し、そのユーザが、過去にライセンスの対価の不払いの実績があるか否かなどを調べ、そのような実

績がない場合には、ライセンスの付与を許容する与信結果を送信し、不払いの実績などがある場合には、ライセンス付与の不許可の与信結果を送信する。

【００９４】ステップＳ１０４において、ライセンスサーバ４のCPU２１は、課金サーバ５からの与信結果が、ライセンスを付与することを許容する与信結果であるか否かを判定し、ライセンスの付与が許容されている場合には、ステップＳ１０５に進み、ライセンスIDに対応するライセンスをデータベースから取り出し、ライセンスの使用規則のフィールドに端末IDを挿入し、ライセンスサーバ４の秘密鍵で電子署名を生成、付加する。

【００９５】そして、ステップＳ１０７に進み、ライセンスサーバ４のCPU２１は、その端末IDと電子署名が付加されたライセンスを通信部２９からインターネット２を介してクライアント１に送信させる。

【００９６】ステップＳ１０８においてライセンスサーバ４のCPU２１は、ステップＳ１０７の処理で、いま送信したライセンスをステップＳ１０２の処理で取り込まれたユーザIDとパスワードに対応して、記憶部２８に記憶させる。さらに、ステップＳ１０９において、CPU２１は、課金処理を実行する。具体的には、CPU２１は、通信部２９から課金サーバ５に、そのユーザIDとパスワードに対応するユーザに対する課金処理を要求する。課金サーバ５は、この課金の要求に基づいて、そのユーザに対する課金処理を実行する。上述したように、この課金処理に対して、そのユーザが支払いを行わなかったような場合には、以後、そのユーザは、ライセンスの付与を要求したとしても、ライセンスを受けることができないことになる。

【００９７】すなわち、この場合には、課金サーバ５からライセンスの付与を不許可とする与信結果が送信されてくるので、ステップＳ１０４からステップＳ１１０に進み、CPU２１は、エラー処理を実行する。具体的には、ライセンスサーバ４のCPU２１は、通信部２９を制御してアクセスしてきたクライアント１に対して、ライセンスを付与することができない旨のメッセージを出力し、処理を終了させる。

【００９８】この場合、上述したように、そのクライアント１はライセンスを受けることができないので、そのコンテンツを利用することができないことになる。

【００９９】次に、図１３を用いてライセンスが利用可能なコンテンツのコンテンツデータを取得する処理を説明する。

【０１００】ユーザが入力部２６を操作し、ライセンスを選択すると、CPUは、通信部２９を制御し、インターネット２を介してコンテンツサーバ３に、選択されたライセンスのライセンスIDを含むコンテンツリスト要求を送信する。ライセンスサーバ４はコンテンツリスト要求を受信すると、コンテンツリスト要求に含まれるライセンスIDを取り出す。ライセンスサーバ４はライセンスIDをキーとしてライセンスデータベースから、該当するライセンスによって利用可能なコンテンツを抽出する。その後、ライセンスサーバは、抽出された各コンテンツのコンテンツID、コンテンツをダウンロードするためのURL、及びコンテンツ名、アーティスト名、ジャンル等のコンテンツ情報を含む、コンテンツリストをクライアント１に送信する。

【０１０１】クライアント１は出力部を制御してコンテンツリストを受信するとコンテンツリストに含まれる各コンテンツのコンテンツ情報を表示させる。ユーザが表示されたコンテンツ情報を参照して、ダウンロードするコンテンツを選択すると、クライアント１はコンテンツのURLに従って、コンテンツサーバにコンテンツ要求をコンテンツサーバ３に送信する。コンテンツサーバはコンテンツ要求を受信すると、コンテンツ要求に含まれるコンテンツIDを持つコンテンツをクライアント１に送信する。クライアント１はコンテンツサーバ３からコンテンツを受信すると、受信したコンテンツを記憶部２８に記憶させる。

【０１０２】以上のようにして、ユーザはライセンスにより利用可能となるコンテンツを探し出し、コンテンツサーバ３からクライアントのダウンロードさせることができる。

【０１０３】図１４は、ブロードキャストインクリプション（Broadcast Encryption）を、キーの管理方式に採用した場合におけるキーの構成方法を表している。図１４に示されるように、キーは、階層ツリー構造とされ、最下段のリーフ（leaf）が個々のデバイスに対応する。図１４の例の場合、番号０から番号１５までの１６個のデバイスに対応するキーが生成される。

【０１０４】各キーは、図中丸印で示される各ノードに対応して規定される。この例では、最上段のルートノードに対応してキーＫＲが、２番目のノードに対応してキーＫ０，Ｋ１が、３段目のノードに対応してキーＫ００乃至Ｋ１１が、第４番目のノードに対応してキーＫ０００乃至キーＫ１１１が、それぞれ対応されている。そして、最下段のノードとしてのリーフ（デバイスノード）に、キーＫ００００乃至Ｋ１１１１が、それぞれ対応されている。

【０１０５】階層構造とされているため、例えば、キーＫ００１０とキー００１１の上位のキーは、Ｋ００１とされ、キーＫ０００とキーＫ００１の上位のキーは、Ｋ００とされている。以下同様に、キーＫ００とキーＫ０１の上位のキーは、Ｋ０とされ、キーＫ０とキーＫ１の上位のキーは、ＫＲとされている。

【０１０６】コンテンツを利用するために用いるキーは、最下段のデバイスノード（リーフ）から、最上段のルートノードまでの１つのパスの各ノードに対応するキーで構成される。例えば、番号３のコンテンツを利用するキーは、キーＫ００１１，Ｋ００１，Ｋ００，Ｋ０，

ＫＲを含むパスの各キーで構成される。

【０１０７】本発明のシステムにおいては、例えば、図15に示されるように、８×２４×３２段のノードに対応するキーで構成される階層ツリー構造キーシステムが利用される。このキーシステムでは、ルートノードから下位の８段までの各ノードに対応するキーに、カテゴリが対応される。ここにおけるカテゴリとは、例えばメモリスティックなどの半導体メモリを使用する機器のカテゴリ、デジタル放送を受信する機器のカテゴリといったカテゴリを意味する。

【０１０８】図15の例では、ルートノードから８段目のノードのうちの１つのノードに、本発明のシステムが対応される。このノードよりさらに下の階層の２４段のノードに対応するキーにより、ライセンスが対応される。これにより、約１６メガ（＝224＝約１６０万）のライセンスを規定することができる。さらに、最も下側の３２段の階層により、約４ギガ（＝232＝約４０億）のユーザを規定することができる。最下段の３２段のノードに対応するキーが、DNK（Device Node Key）を構成する。

【０１０９】各コンテンツは、６４（＝８＋２４＋３２）段の各ノードで構成されるパスの内の１つに対応される。すなわち、各コンテンツの暗号化には、割り当てられたパスを構成するノードに対応するキーが用いられる。上位の階層のキーは、その直近の下位の階層のキーを用いて暗号化され、図５のＥＫＢ内に配置される。最下段のＤＮＫは、ＥＫＢ内には配置されず、クライアントがライセンスサーバに登録するときに取得するサービスデータに記述され、図16に示されるように、ユーザのクライアント１に与えられる。

【０１１０】クライアント１は、サービスデータに記述されているＤＮＫを用いて、コンテンツデータとともに配布されるＥＫＢ内に記述されている直近の上位の階層のキーを復号し、復号して得たキーを用いて、ＥＫＢ内に記述されているさらにその上の階層のキーを復号する。以上の処理を順次行うことで、クライアント１は、そのコンテンツのパスに属するすべてのキーを得ることができる。

【０１１１】クライアント１は以上のEKBの復号処理を行った後得られるKRを用いて、KRによって暗号化されているコンテンツキーKR(KC)を復号し、コンテンツキーKCを得ることができる。

【０１１２】なお、本発明におけるキーは、図14および図15に示されるようなブロードキャストインクリプションを利用したキーシステム以外のキーで構成することも可能である。

【０１１３】また、本発明が適用されるクライアントは、いわゆるパーソナルコンピュータ以外に、PDA（Personal Digital Assistants）、携帯電話機、ゲーム端末機などとすることができる。

【０１１４】一連の処理をソフトウエアにより実行させる場合には、そのソフトウエアを構成するプログラムが、専用のハードウエアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどに、ネットワークや記録媒体からインストールされる。

【０１１５】この記録媒体は、図２に示すように、装置本体とは別に、ユーザにプログラムを提供するために配布される、プログラムが記録されている磁気ディスク４１（フロッピディスクを含む）、光ディスク４２（CD-ROM(Compact Disk-Read OnlyMemory),DVD(Digital Versatile Disk)を含む）、光磁気ディスク４３（ＭＤ（Mini-Disk）を含む）、もしくは半導体メモリ４４などよりなるパッケージメディアにより構成されるだけでなく、装置本体に予め組み込まれた状態でユーザに提供される、プログラムが記録されているROM２２や、記憶部２８に含まれるハードディスクなどで構成される。

【０１１６】なお、本明細書において、記録媒体に記録されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

【０１１７】また、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

【０１１８】

【発明の効果】以上の如く、本発明の情報処理装置および方法、プログラム格納媒体、並びにプログラムによれば、暗号化されたデータとコンテンツの属性情報を、所定のフォーマットにフォーマット化して、出力するようにし、ライセンスに属性条件をふ含むようにし、コンテンツの属性情報がライセンスの属性条件を満たす場合に暗号化されたデータを復号できるようにしたので、データが不正に利用されるのを抑制しつつ、ライセンスを柔軟に発行することが可能となる。

【図面の簡単な説明】

【図１】本発明を適用したコンテンツ提供システムの構成を示すブロック図である。

【図２】図１のクライアントの構成を示すブロック図である。

【図３】図１のクライアントのコンテンツのダウンロード処理を説明するフローチャートである。

【図４】図１のコンテンツサーバのコンテンツ提供処理を説明するフローチャートである。

【図５】データフォーマットの例を示す図である。

【図６】属性項目の種類を説明する図である。

【図７】ライセンスの構成を示す図である。

【図８】クライアントの再生処理を説明するフローチャートである。

【図９】ライセンス取得処理を説明するフローチャートである。
【図１０】ライセンス取得処理を説明するフローチャートである。
【図１１】ライセンス取得処理を説明するフローチャートである。
【図１２】ライセンス取得処理の詳細を説明するフローチャートである。
【図１３】コンテンツデータを取得する処理を説明するフローチャートである。
【図14】キーの構成を説明する図である。
【図15】キーの構成とライセンスの関係を説明する図である。
【図16】ライセンスサーバのライセンス付与処理を説明する図である。
【符号の説明】
１－１，１－２　クライアント，　２　インターネット，　３　コンテンツサーバ，　４　ライセンスサーバ，　５　課金サーバ，　２０　タイマ，　２１CPU，　２４　暗号化復号部，　２５　コーデック部，　２６　入力部，　２７出力部，　２８　記憶部，　２９　通信部

【図１】

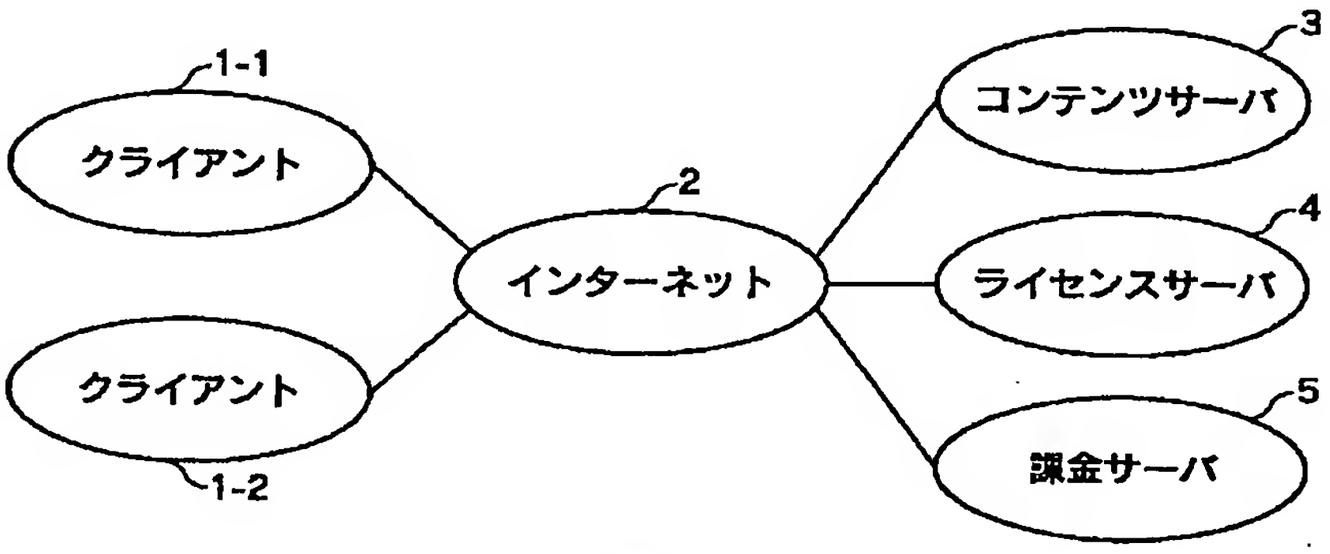

図１

【図２】

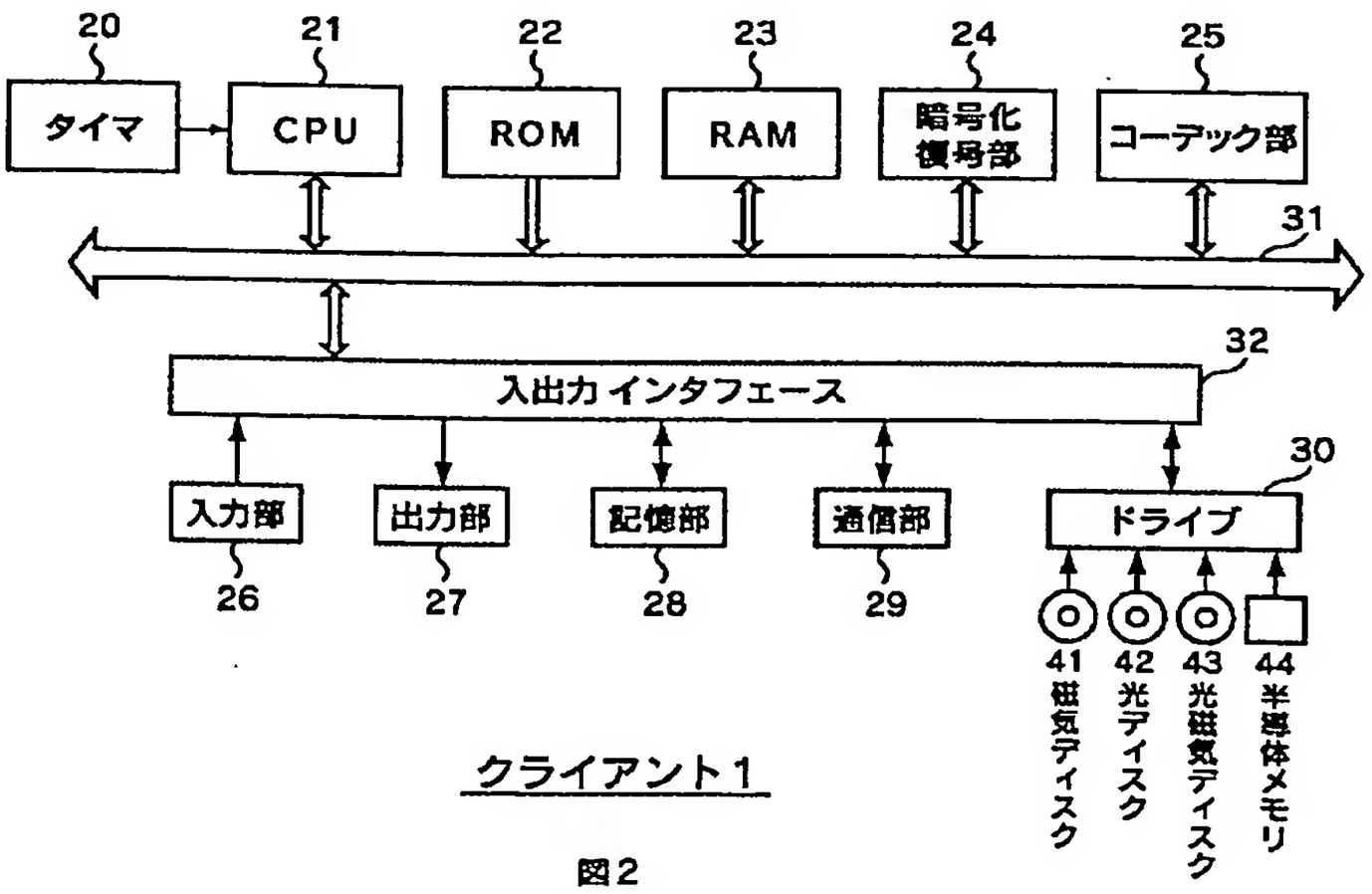

図２

【図３】

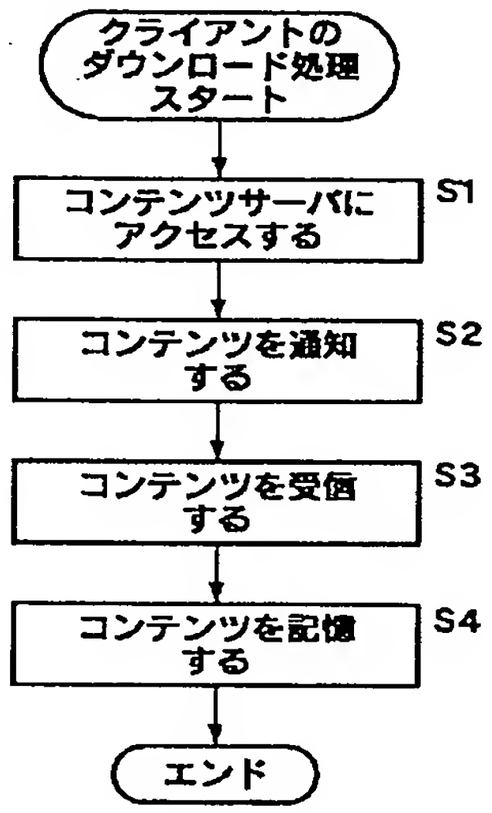

図３

【図７】

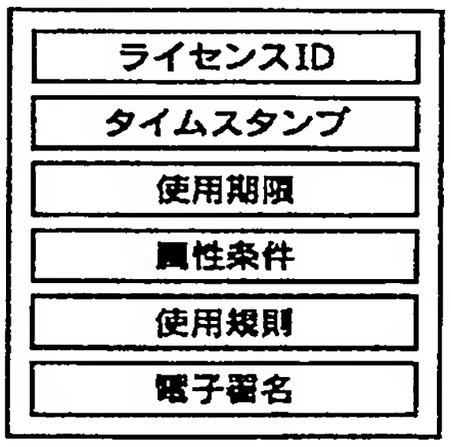

図７

【図４】

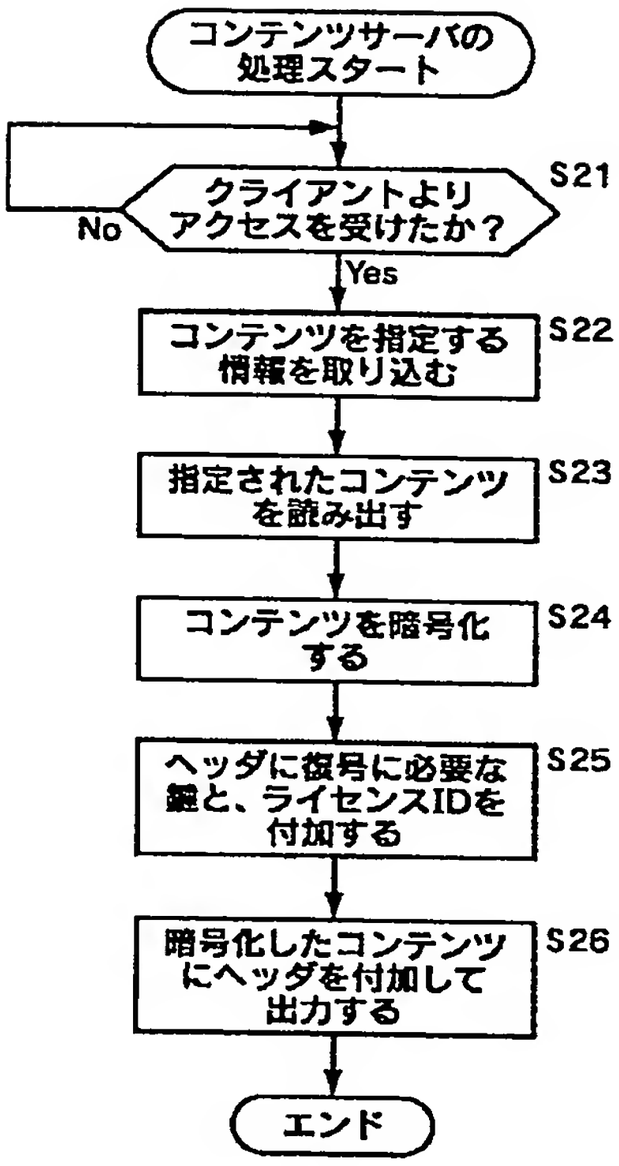

図４

【図５】

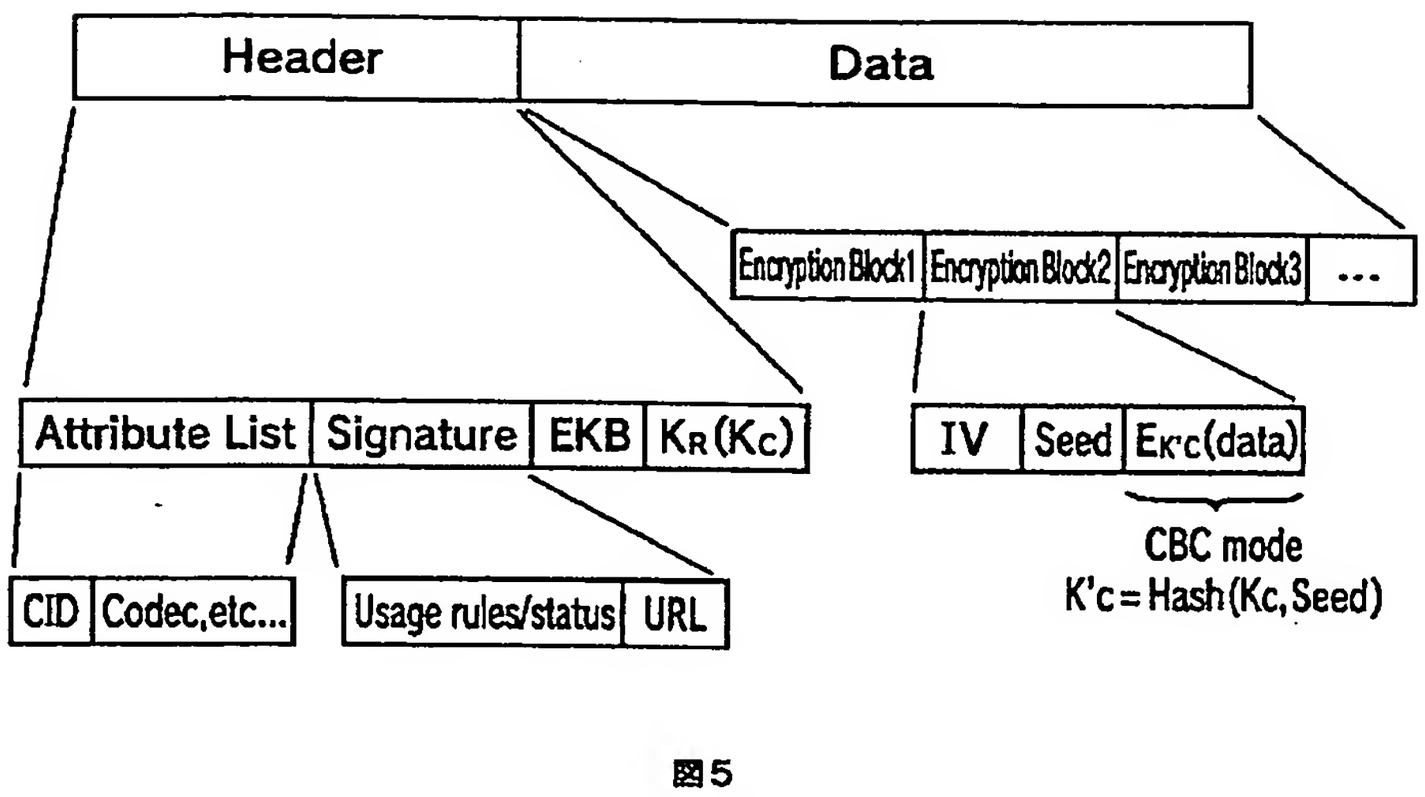

図５

【図６】

属性項目	説明
CID	コンテンツID
RCID	レコード会社ID
CIID	コンテンツ発行者ID
AID	アーティストID
RelDate	リリース日
GID	ジャンルID
LID	レーベルID
SID	サブスクリプションID
URL	ライセンスサーバのURL

図６

【図８】

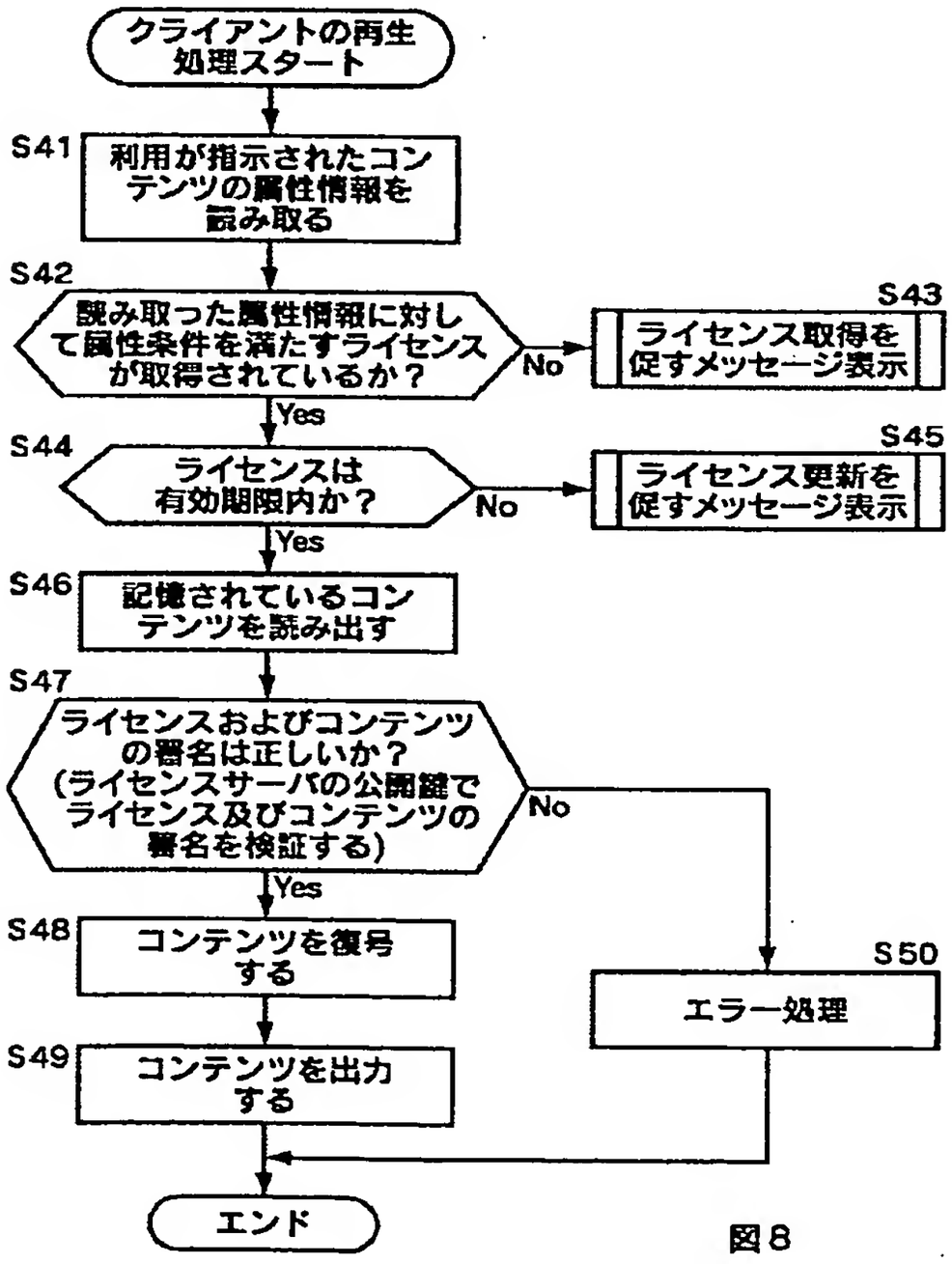

図８

【図９】

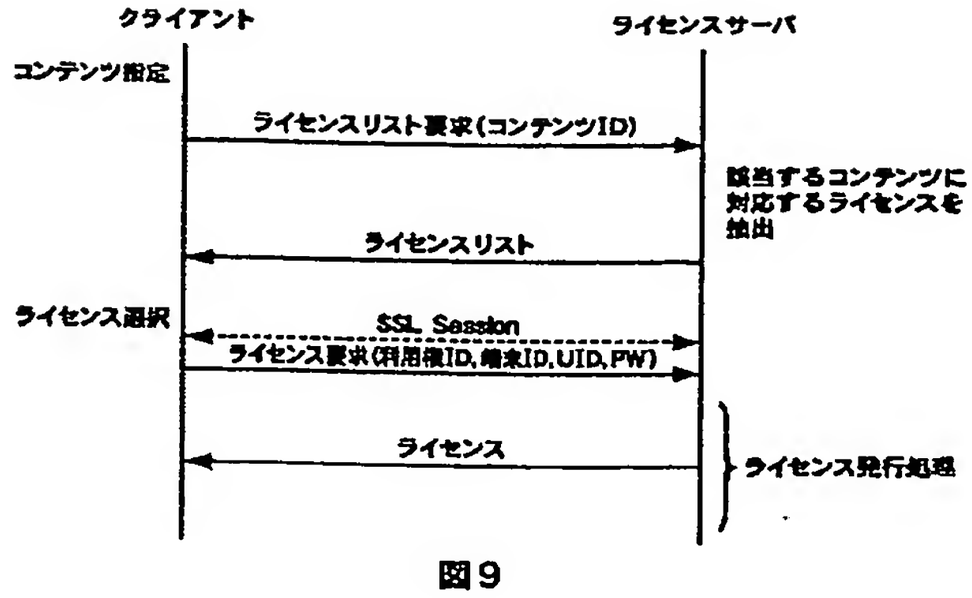

図9

【図１０】

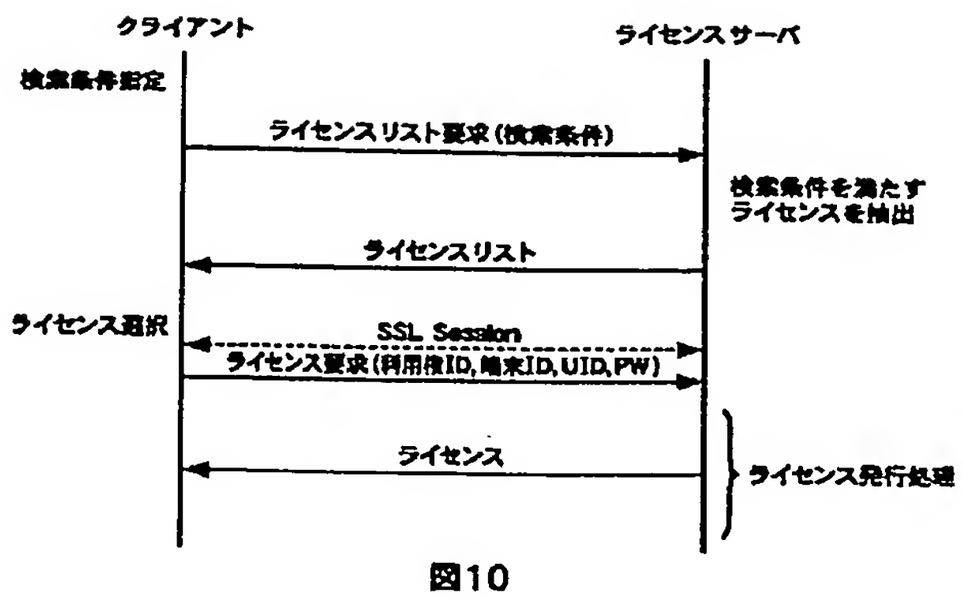

図10

【図１１】

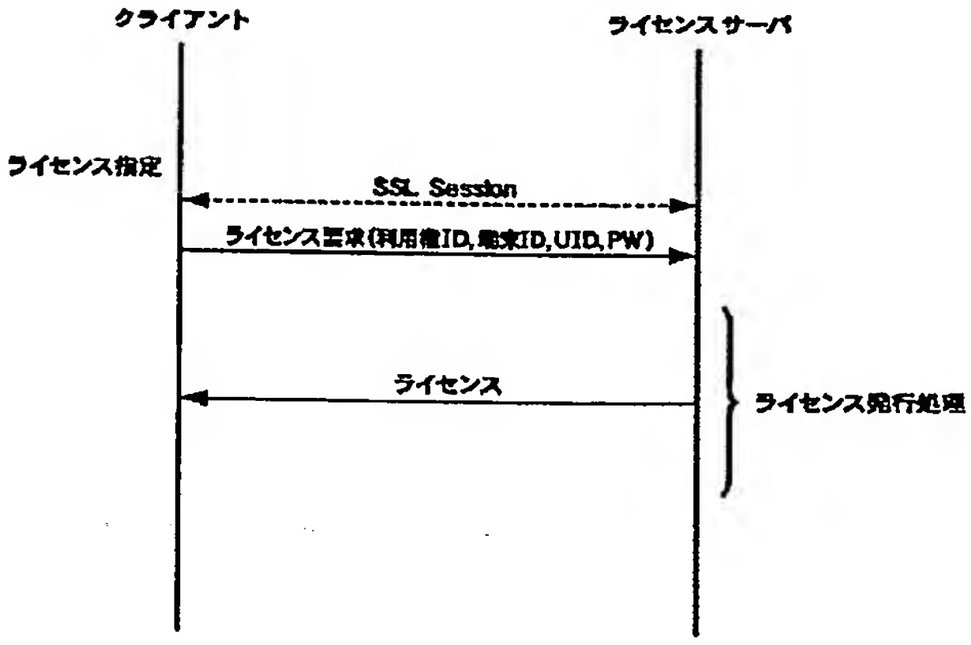

図11

【図１２】

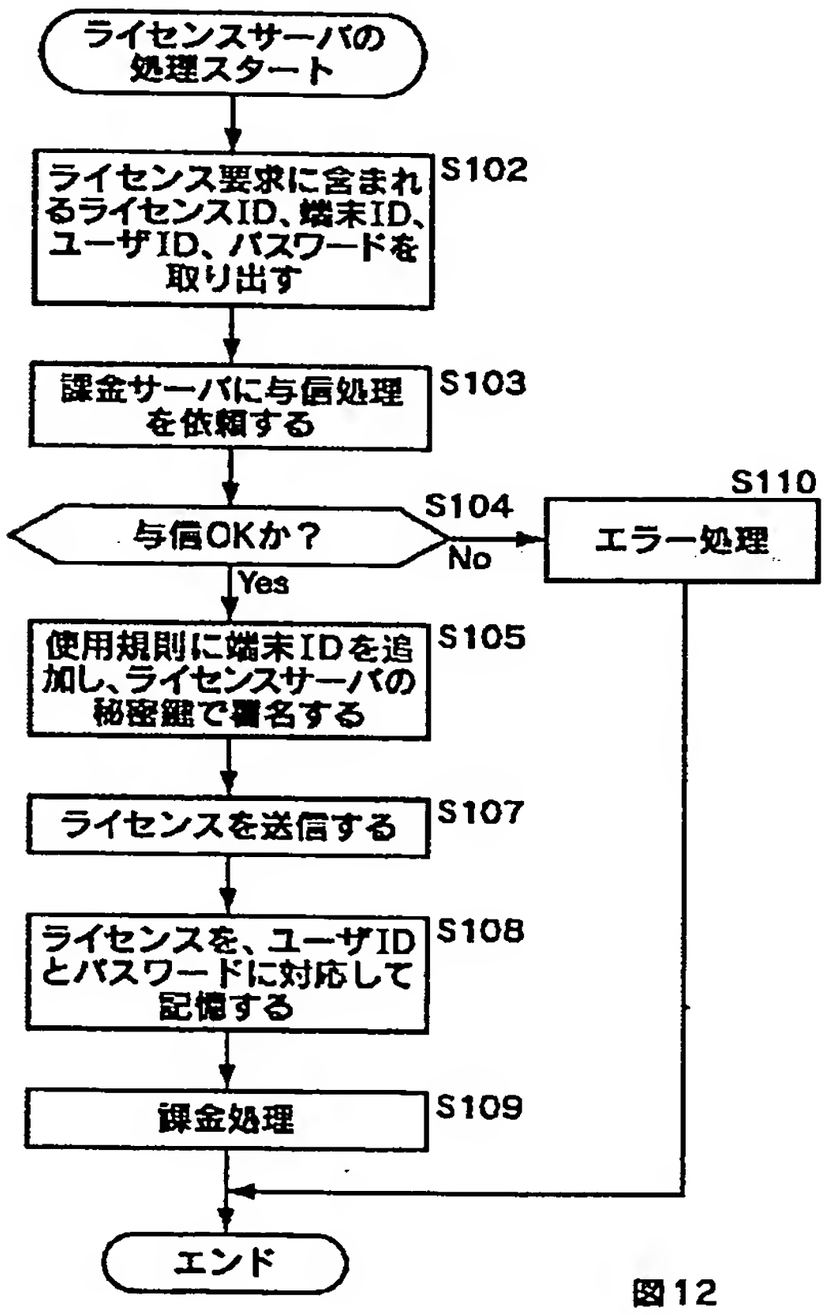

図12

【図１３】

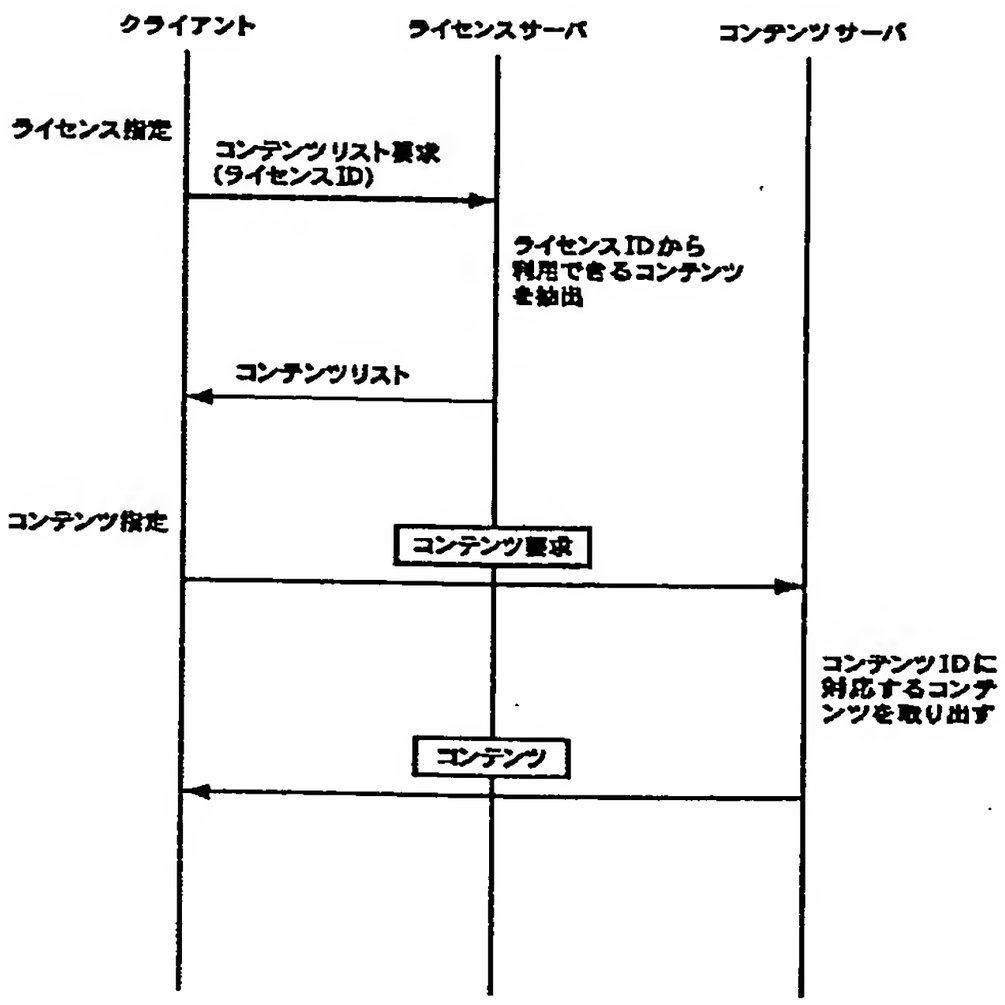

図13

【図１５】

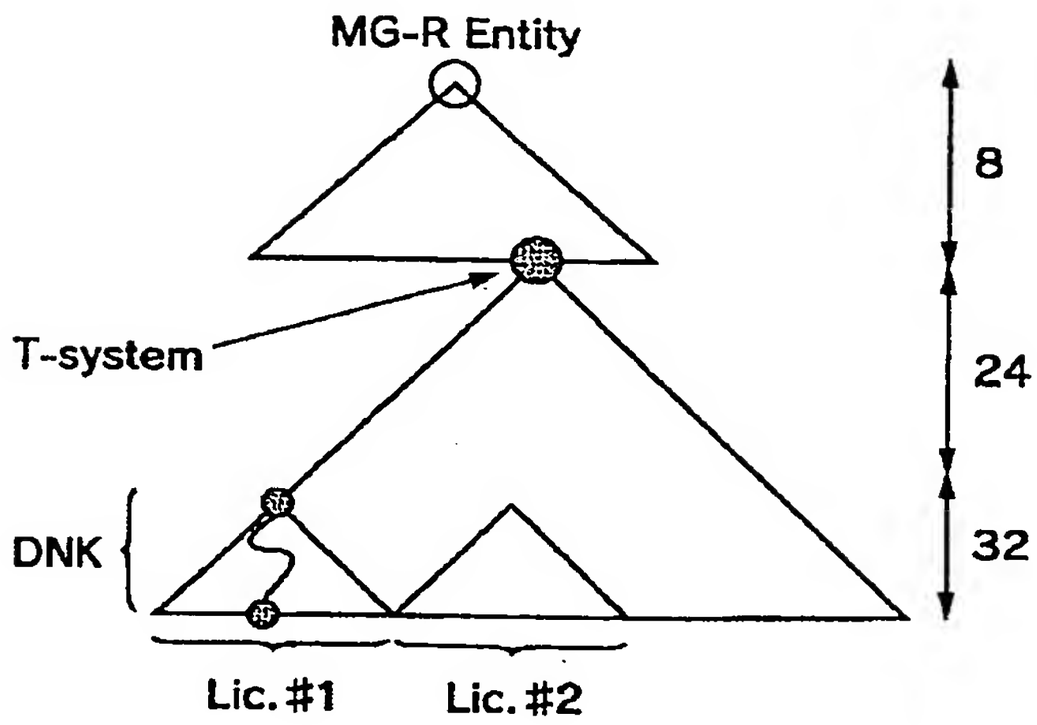

図15

【図１４】

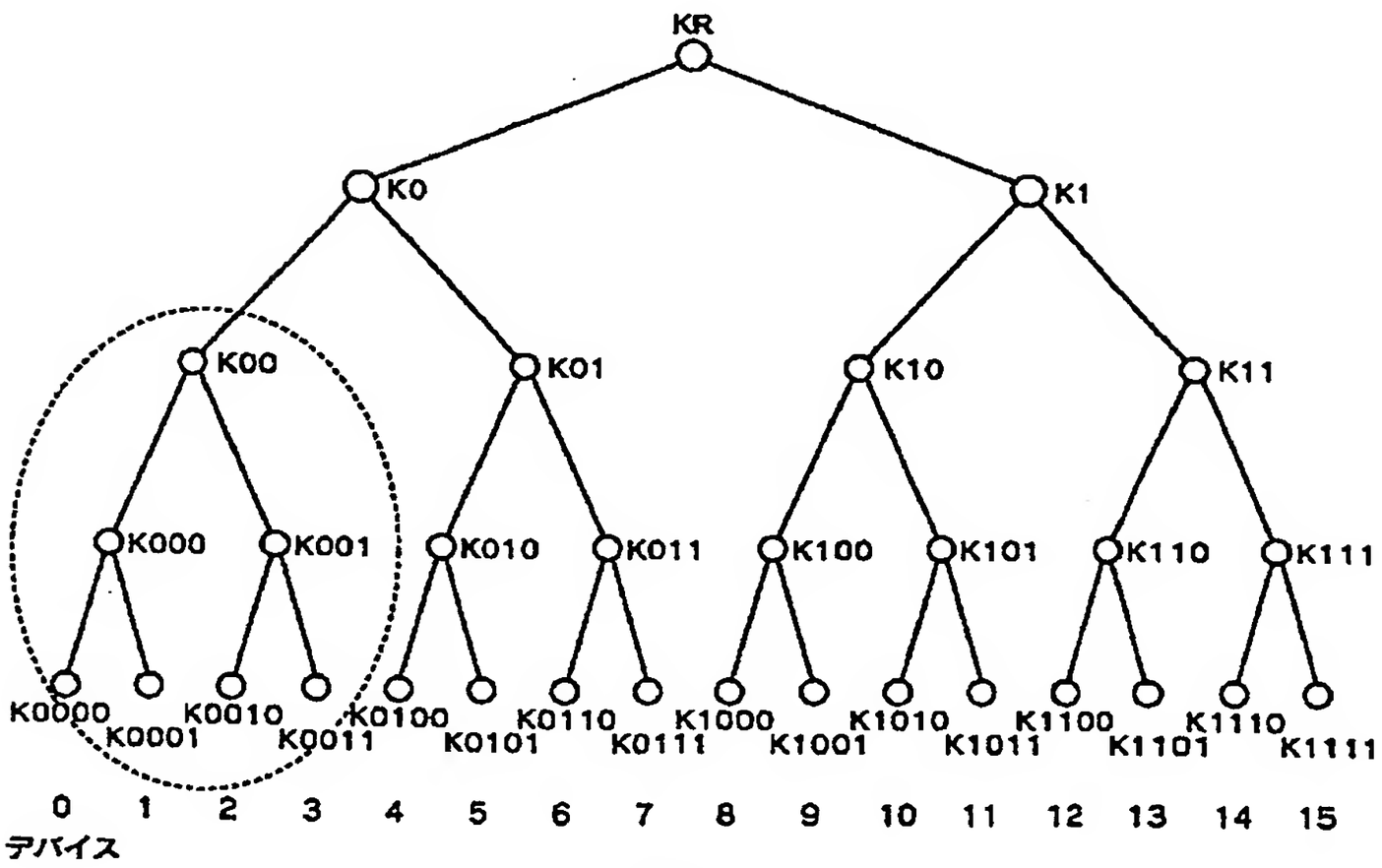

図14

【図１６】

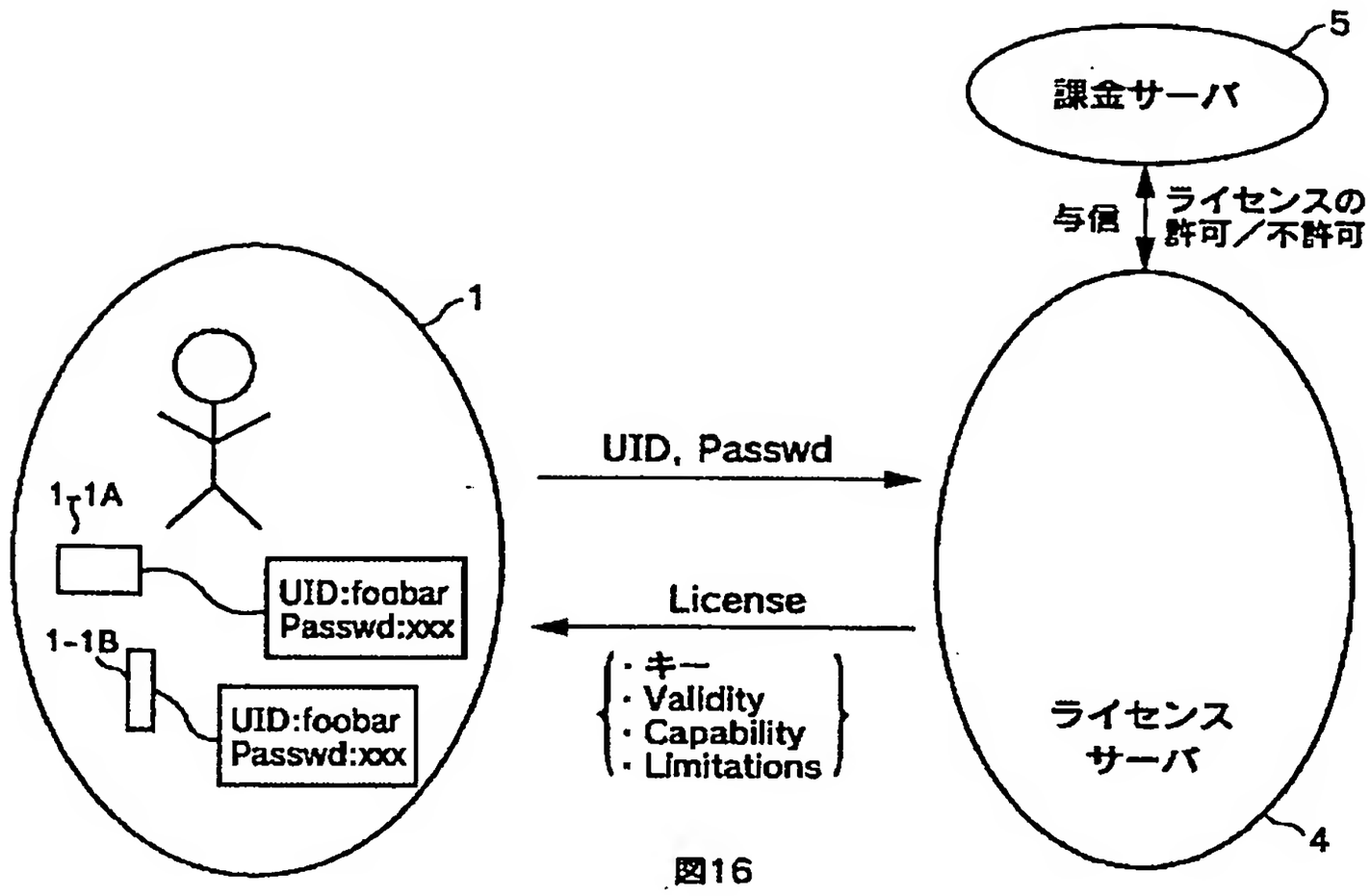

図16

【手続補正書】
【提出日】平成１５年３月１３日（２００３．３．１３）
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正内容】
【特許請求の範囲】
【請求項１】　暗号化コンテンツデータと属性情報とを含むコンテンツを受信するコンテンツ受信手段と、
前記コンテンツを記憶するコンテンツ記憶手段と、
利用できるコンテンツの前記属性情報に関する条件を記載した属性条件を含むライセンスを受信するライセンス受信手段と、
前記ライセンスを記憶するライセンス記憶手段と、
前記コンテンツの前記属性情報が、前記ライセンス記憶手段に記憶されているライセンスの属性条件を満たすか否かを判定する判定手段と、
前記判定手段が前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすと判定したことに基づいて、前記コンテンツの前記暗号化コンテンツデータを復号する復号手段と、
前記復号手段により復号されたコンテンツデータを出力する出力手段とを備えることを特徴とする情報処理装置。
【請求項２】　前記コンテンツは、更に前記コンテンツデータを復号するためのコンテンツキーを含むことを特徴とする請求項１に記載の情報処理装置。
【請求項３】　前記属性情報は、属性項目と属性値の組み合わせからなることを特徴とする請求項１に記載の情報処理装置。
【請求項４】　前記属性項目はレコード会社、アーティスト、リリース日、コンテンツ発行者、ジャンル、サブスクリプション、またはレーベルに関する情報を含むことを特徴とする請求項１に記載の情報処理装置。
【請求項５】　前記属性条件は属性項目、属性値、及び演算子の組み合わせからなることを特徴とする請求項１に記載の情報処理装置。
【請求項６】　コンテンツに含まれる属性情報に関する条件を記載した属性条件を含むライセンスを一意に識別するライセンスIDを含むライセンス要求を受信する受信手段と、
ライセンスをライセンスIDと共に記憶する記憶手段と、
前記ライセンス要求に含まれる前記ライセンスIDに対応する前記ライセンスを取り込む取り込み手段と、
前記ライセンスに電子署名を付加する署名手段と、
署名手段により署名されたライセンスを送信する送信手段とを備えることを特徴とする情報処理装置。
【請求項７】　更に、前記取り込み手段によって取り込まれたライセンスに端末IDを付加するライセンス処理手段を備えることを特徴とする請求項６に記載の情報処理装置。
【請求項８】　暗号化コンテンツデータと属性情報とを含むコンテンツを記憶する記憶手段と、

コンテンツを一意に識別するコンテンツIDを含むコンテンツ要求を受信する受信手段と、
コンテンツ要求に含まれるコンテンツIDに対応するコンテンツを送信する送信手段と、
を備える情報処理装置であって、
前記コンテンツに含まれる前記属性情報は、当該コンテンツを利用する際にライセンスの属性条件を満たすか否かを判断するために用いられる情報であり、
前記ライセンスの属性条件は利用できる前記コンテンツの前記属性情報に関する条件を記載した情報であることを特徴とする情報処理装置。
【請求項９】　暗号化コンテンツデータと属性情報とを含むコンテンツを受信するコンテンツ受信ステップと、
前記コンテンツを記憶するコンテンツ記憶ステップと、
利用できるコンテンツの前記属性情報に関する条件を記載した属性条件を含むライセンスを受信するライセンス受信ステップと、
前記ライセンスを記憶するライセンス記憶ステップと、
前記コンテンツの前記属性情報が、前記ライセンス記憶ステップの処理により記憶されたライセンスの属性条件を満たすか否かを判定する判定ステップと、
前記判定手段が前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすと判定したことに基づいて、前記コンテンツの前記暗号化コンテンツデータを復号する復号ステップと、
前記復号手段により復号されたコンテンツデータを出力する出力ステップとを含むことを特徴とする情報処理方法。
【請求項１０】　暗号化コンテンツデータと属性情報とを含むコンテンツを受信するコンテンツ受信ステップと、
前記コンテンツを記憶するコンテンツ記憶ステップと、
利用できるコンテンツの前記属性情報に関する条件を記載した属性条件を含むライセンスを受信するライセンス受信ステップと、
前記ライセンスを記憶するライセンス記憶ステップと、
前記コンテンツの前記属性情報が、前記ライセンス記憶ステップの処理により記憶されたライセンスの属性条件を満たすか否かを判定する判定ステップと、
前記判定手段が前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすと判定したことに基づいて、前記コンテンツの前記暗号化コンテンツデータを復号する復号ステップと、
前記復号手段により復号されたコンテンツデータを出力する出力ステップとをコンピュータに実行させるプログラム。
【請求項１１】　暗号化コンテンツデータと属性情報とを含むコンテンツを受信するコンテンツ受信ステップと、
前記コンテンツを記憶するコンテンツ記憶ステップと、
利用できるコンテンツの前記属性情報に関する条件を記載した属性条件を含むライセンスを受信するライセンス受信ステップと、
前記ライセンスを記憶するライセンス記憶ステップと、
前記コンテンツの前記属性情報が、前記ライセンス記憶ステップの処理により記憶されたライセンスの属性条件を満たすか否かを判定する判定ステップと、
前記判定手段が前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすと判定したことに基づいて、前記コンテンツの前記暗号化コンテンツデータを復号する復号ステップと、
前記復号手段により復号されたコンテンツデータを出力する出力ステップとをコンピュータに実行させるプログラムが格納されたプログラム格納媒体。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】０００８
【補正方法】変更
【補正内容】
【０００８】
【課題を解決するための手段】本発明の第１の情報処理装置は、暗号化コンテンツデータと属性情報とを含むコンテンツを受信するコンテンツ受信手段と、前記コンテンツを記憶するコンテンツ記憶手段と、利用できるコンテンツの前記属性情報に関する条件を記載した属性条件を含むライセンスを受信するライセンス受信手段と、前記ライセンスを記憶するライセンス記憶手段と、前記コンテンツの前記属性情報が、前記ライセンス記憶手段に記憶されているライセンスの属性条件を満たすか否かを判定する判定手段と、前記判定手段が前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすと判定したことに基づいて、前記コンテンツの前記暗号化コンテンツデータを復号する復号手段と、前記復号手段により復号されたコンテンツデータを出力する出力手段とを備えることを特徴とする。
【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】００１１
【補正方法】変更
【補正内容】
【００１１】前記属性項目はレコード会社、アーティスト、リリース日、コンテンツ発行者、ジャンル、サブスクリプション、またはレーベルに関する情報を含むようにすることができる。
【手続補正４】
【補正対象書類名】明細書
【補正対象項目名】００１６
【補正方法】変更
【補正内容】
【００１６】本発明の情報処理方法は、暗号化コンテン

ツデータと属性情報とを含むコンテンツを受信するコンテンツ受信ステップと、前記コンテンツを記憶するコンテンツ記憶ステップと、利用できるコンテンツの前記属性情報に関する条件を記載した属性条件を含むライセンスを受信するライセンス受信ステップと、前記ライセンスを記憶するライセンス記憶ステップと、前記コンテンツの前記属性情報が、前記ライセンス記憶ステップの処理により記憶されたライセンスの属性条件を満たすか否かを判定する判定ステップと、前記判定手段が前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすと判定したことに基づいて、前記コンテンツの前記暗号化コンテンツデータを復号する復号ステップと、前記復号手段により復号されたコンテンツデータを出力する出力ステップとを含むことを特徴とする。

【手続補正５】
【補正対象書類名】明細書
【補正対象項目名】００１７
【補正方法】変更
【補正内容】
【００１７】本発明のプログラムは、暗号化コンテンツデータと属性情報とを含むコンテンツを受信するコンテンツ受信ステップと、前記コンテンツを記憶するコンテンツ記憶ステップと、利用できるコンテンツの前記属性情報に関する条件を記載した属性条件を含むライセンスを受信するライセンス受信ステップと、前記ライセンスを記憶するライセンス記憶ステップと、前記コンテンツの前記属性情報が、前記ライセンス記憶ステップの処理により記憶されたライセンスの属性条件を満たすか否かを判定する判定ステップと、前記判定手段が前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすと判定したことに基づいて、前記コンテンツの前記暗号化コンテンツデータを復号する復号ステップと、前記復号手段により復号されたコンテンツデータを出力する出力ステップとをコンピュータに実行させるプログラムである。

【手続補正６】
【補正対象書類名】明細書
【補正対象項目名】００１８
【補正方法】変更
【補正内容】
【００１８】本発明のプログラム格納媒体に格納されているプログラムは、暗号化コンテンツデータと属性情報とを含むコンテンツを受信するコンテンツ受信ステップと、前記コンテンツを記憶するコンテンツ記憶ステップと、利用できるコンテンツの前記属性情報に関する条件を記載した属性条件を含むライセンスを受信するライセンス受信ステップと、前記ライセンスを記憶するライセンス記憶ステップと、前記コンテンツの前記属性情報が、前記ライセンス記憶ステップの処理により記憶されたライセンスの属性条件を満たすか否かを判定する判定ステップと、前記判定手段が前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすと判定したことに基づいて、前記コンテンツの前記暗号化コンテンツデータを復号する復号ステップと、前記復号手段により復号されたコンテンツデータを出力する出力ステップとをコンピュータに実行させるプログラムである。

【手続補正７】
【補正対象書類名】明細書
【補正対象項目名】００７８
【補正方法】変更
【補正内容】
【００７８】ステップＳ４４において、ライセンスはまだ有効期限内であると判定された場合、または、ステップＳ４５において、ライセンスが更新された場合、ステップＳ４５に進み、CPU２１は、コンテンツのヘッダに含まれる電子署名及びライセンスに含まれる電子署名をライセンスサーバ４の公開鍵で検証する。電子署名の検証の結果、電子署名が正しいと判断された場合、ステップＳ４６に進み、CPU２１は、暗号化されているコンテンツデータを記憶部２８から読み出し、RAM２３に格納させる。そして、ステップＳ４７において、CPU２１は、RAM２３に記憶された暗号化ブロックのデータを、図５のデータに配置されている暗号化ブロック単位で、暗号化復号部２４に供給し、復号させる。

【手続補正８】
【補正対象書類名】明細書
【補正対象項目名】００８０
【補正方法】変更
【補正内容】
【００８０】図９乃至図１１を用いてクライアントがライセンスサーバ４からライセンスを取得する処理を説明する。

【手続補正９】
【補正対象書類名】明細書
【補正対象項目名】００９１
【補正方法】変更
【補正内容】
【００９１】図１２のフローチャートを参照して、図９乃至図１１におけるライセンス発行処理の詳細を説明する。なお、この場合においても、図２のクライアント１の構成は、ライセンスサーバ４の構成としても引用される。

【手続補正１０】
【補正対象書類名】明細書
【補正対象項目名】０１０８
【補正方法】変更
【補正内容】
【０１０８】図１５の例では、ルートノードから８段目のノードのうちの１つのノードに、本発明のシステムが対応される。このノードよりさらに下の階層の２４段の

ノードに対応するキーにより、ライセンスが対応される。これにより、約１６メガ（＝2^{24}＝約１６０万）のライセンスを規定することができる。さらに、最も下側の３２段の階層により、約４ギガ（＝2^{32}＝約４０億）のユーザを規定することができる。最下段の３２段のノードに対応するキーが、DNK（Device Node Key）を構成する。

【手続補正１１】
【補正対象書類名】図面
【補正対象項目名】図４
【補正方法】変更
【補正内容】
【図４】

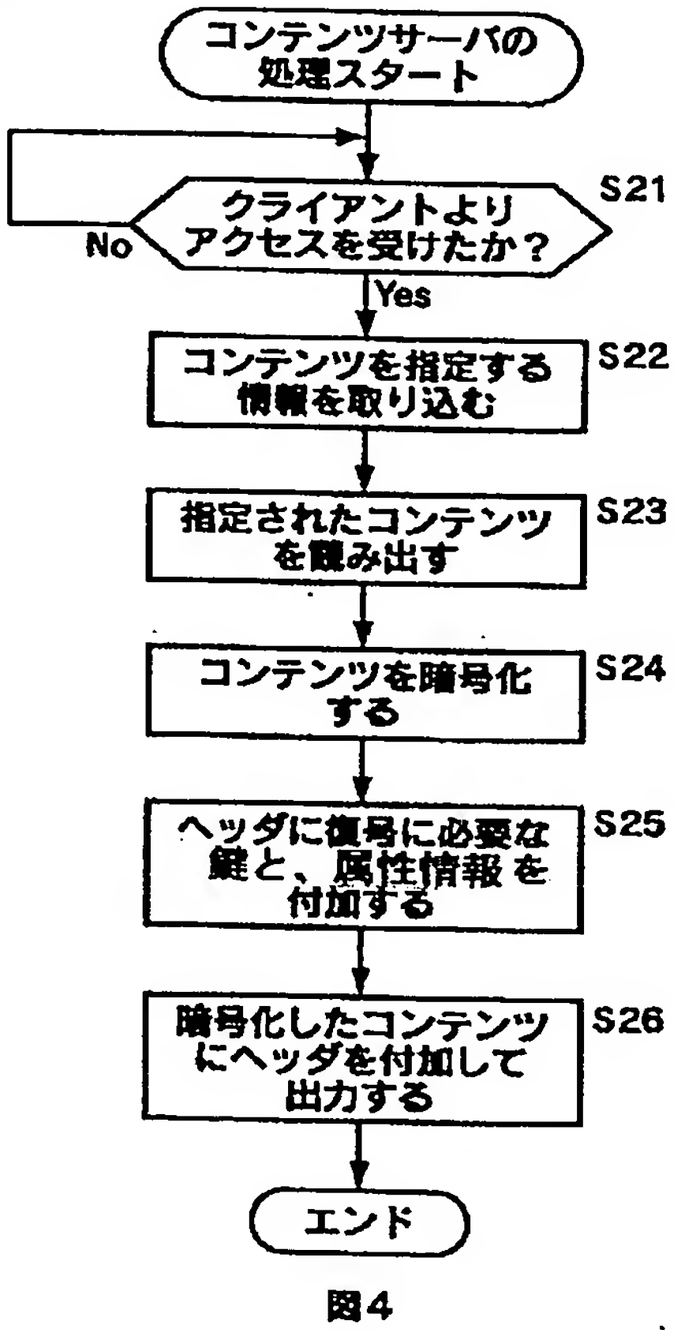

図4